



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/645,375

08/20/2003

Keith Ballinger

13768.454

7425

47973 7590 01/16/2008
WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER

SAN JUAN, MARTINJERIKO P

ART UNIT

PAPER NUMBER

2132

MAIL DATE

DELIVERY MODE

01/16/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/645,375

Applicant(s)

BALLINGER ET AL.

Examiner

Martin Jeriko P. San Juan

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5-14, 17-24, 26-29 and 32-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5-14, 17-24, 26-29, and 32-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input checked="" type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. <u>20071030</u> . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This is a response to Applicant's Amendments filed on October 30, 2007.

Claims 1-31 were originally pending.

Claims 1-3, 5-8, 10-11, 14-19, 21-22, and 28-31 were rejected; and 4, 9, 12-13, 20, and 23-27 were allowed on the first action filed on January 8, 2007.

Claims 1, 6, 14, 17, 19, 26, and 29 have been amended to incorporate allowable subject matter; claims 4, 15-16, 25, and 30-31 have been cancelled; new claims 32-33 have been added by the Applicant.

Claims 1-3, 5-14, 17-24, 26-29, and 32-33 were rejected on July 30, 2007.

Claims 1, 14, 17, and 29 have been amended. New claims 34 and 35 have been added.

Claims 1-3, 5-14, 17-24, 26-29, and 32-35 are currently pending.

Response to Arguments

1. Applicant's arguments, see Remarks and Amendments, filed October 30, 2007, with respect to the rejection(s) of claim(s) 1, 14, 17, and 29 under 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Fieres et al. [US 6178504 B1].

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claims 29 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

a. The limitation regarding the act of converting the token data for the outbound token collection using a private key that is only accessible by the sending computer system and a receiving computer system contains the new subject matter. Specifically, the private key being only accessible by the sending computer system and a receiving computer system is not supported.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-3, 5-7, and 14 are rejected under 35 U.S.C. 102(b) as being anticipated by Fieres et al. [US 6178504 B1], hereinafter Fieres.

Regarding claim 1, Fieres teaches in a computerized network environment including two or more computer systems sending messages through a network [US 6178504 B1, Col 11, Ln 39-61 --Examiner notes Application requesting services of handling enterprise critical data, and consumer private data.], a method of receiving [US 6178504 B1, Col 10, Ln 25-36] secure messages [US 6178504 B1, Col 4, Ln 21-25 --Examiner notes encrypted messages are evidently secure messages.] using custom security tokens [US 6178504 B1, Col 4, Ln 48-58] [US 6178504 B1, Col 6, Ln 26-46], the method comprising: an act of identifying one or more security tokens [US 6178504 B1, Col 6, Ln 26-30] in a received message that has been encrypted [US 6178504 B1, Col 4, Ln 21-25 --Examiner notes client/server Application requests contains or is the secure message.], and a value type corresponding with each identified security token [US 6178504 B1, Col 12, Ln 29-35]; an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access [US 6178504 B1, Col 12, Ln 15-28], wherein the stored value type comprises a collection of executable instructions for data handling [US 6178504 B1, Col 13, Ln 6-32]; an act of receiving data from the at least one identified security token into the stored value type that has been matched [US 6178504 B1, Col 6, Ln 26-38], wherein the raw data includes a custom property, wherein the custom property defines one or more of time of day, geographic location, limitations on message access, or

limitations on device access [US 6178504 B1, Col 6, Ln 30 –Examiner notes an Application ID contained in a certificate reads on a custom property which defines limitations on message access through classes of services.] [US 6178504 B1, Col 13, Ln 24-32 –Examiner notes COS attributes such as number of usage or expiration time all reading on custom properties.]; and an act of decrypting an encrypted portion of the received message [US 6178504 B1, Col 11, Ln 30-37] and accessing the received message based at least in part on the raw data, including the custom property, received from the at least one identified security token [US 6178504 B1, Col 11, Ln 55-55-56].

Regarding claim 2, Fieres teaches the method as recited in claim 1, wherein the received message includes one or more digital signatures, the method further comprising an act of authenticating at least one of the one or more digital signatures [US 6178504 B1, Col 10, Ln 25-44].

Regarding claim 3, Fieres teaches the method as recited in claim 1, further comprising an act of receiving a message from a sending computer system, the message including an encrypted portion and one or more security tokens [US 6178504 B1, Col 4, Ln 21-25].

Claim 4 is cancelled.

Regarding claim 5, Fieres teaches the method as recited in claim 1, wherein the at least one identified security token is a binary security token [US 6178504 B1, Col 6, Ln 28 – Examiner notes that digital certificates read on binary security tokens.].

Regarding claim 6, Fieres teaches the method as recited in claim 1, wherein the identified corresponding value type is a custom value type created by the sending computer system or the receiving computer system, and that the receiving and sending computer system can access [US 6178504 B1, Col 14, Table 1].

Regarding claim 7, Fieres teaches the method as recited in claim 1, further comprising an act of updating one or more properties of the stored security token that is accessible by the receiving computer system with one or more of the identification information and the custom property [US 6178504 B1, Col 13, Ln 24-32 –Examiner notes COS attributes such as number of usage or expiration time all reading on custom properties.] [US 6178504 B1, Col 19, Ln 12-35 —Examiner notes digital signature (identification information) is evidently updated.]

Regarding claim 14, Fieres teaches in a computerized network environment including two or more computer systems sending messages through a network communication protocol, a method of receiving secure messages using custom security tokens, the method comprising: an act of at a receiving computer system [US 6178504 B1, Fig 7 -- Examiner notes Server receiving Application requests from Client.] identifying one or

more security tokens in a received message [US 6178504 B1, Col 6, Ln 26-30], from a sending computer system [Examiner notes Client reads on the "sending computer system."], that has been encrypted [US 6178504 B1, Col 4, Ln 21-25], and a value type corresponding with each identified security token [US 6178504 B1, Col 13, Ln 33-35 and Col 13, Ln 42-44], wherein the identified value type is a custom program class that only the receiving computer system and the sending computer system can access [US 6178504 B1, Col 13, Ln 33-35 and Col 13, Ln 42-44 –Examiner notes that program codes/agents for execution read on program class.]; an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access [US 6178504 B1, Col 12, Ln 15-28]; and an act of receiving data from the at least one identified security token into the stored value type that has been matched [US 6178504 B1, Col 6, Ln 26-38], wherein the raw data includes one or more of identification information, and a custom property [US 6178504 B1, Col 6, Ln 30] [US 6178504 B1, Col 13, Ln 24-32] [US 6178504 B1, Col 19, Ln 12-35]; and an act of decrypting an encrypted portion of the received message based at least in part on the raw data received from the at least one identified security token [US 6178504 B1, Col 11, Ln 21-24].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

1. Claim 8-13, 17-24, 26-29, and 32-35 rejected under 35 U.S.C. 103(a) as being unpatentable over Fieres et al. [US 6178504 B1], hereinafter Fieres, and further in view of de Jong et al. [US Pub No. 2004/0054628 A1], hereinafter de Jong.

Regarding claim 8, Fieres teaches the method as recited in claim 7. However, Fieres does not teach further comprising an act of creating a security key when updating the one or more properties of the stored security token.

De Jong teaches an act of updating one or more properties of a stored security token further comprising an act of creating a security key when updating the one or more properties of the stored security token [A token chain key is created when a new token chain is being generated because of updated token properties/specifications/parameters. A token pool key is also created when new tokens or token chains or token pools are generated. (US 2004/0054628 A1, Pg 10, Par 0140) (US 2004/0054628 A1, Fig 20)].

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the digital content access control of de Jong into the invention of Fieres. The suggestion/motivation would have been to have an invention capable of controlling both application resources and digital content especially when a digital content may require the use of a specific application resource. Fieres and de Jong are analogous because they are both in the same field of endeavor of controlling access in a digital network through the use of security tokens.

Regarding claim 9, the combined inventions of Fieres and de Jong teach the method as recited in claim 1, wherein the identified at least one security token is serialized in the received message based on a private key that is shared between the sending and receiving computer system [Token chain keys are shared between sending and receiving entities of authenticated digital content requests. (US 2004/0054628 A1, Pg 11, Par 0152)].

Regarding claim 10, the combined inventions of Fieres and de Jong teach the method as recited in claim 9, wherein the private key is accessed from a key provider that both the sending and the receiving computer systems can access [The Synchronizer is the key provider and synchronization of token pool information that can be accessed by sending and receiving authenticated digital content request entities through internal requests for synchronization (US 2004/0054628 A1, Pg 18, Par 0213)].

Regarding claim 11, the method as recited in claim 1, wherein the one or more security tokens are found in a security header portion of the message are inherent when using Web Services Security communications protocol as taught by the combined inventions of Fieres and de Jong [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 12, the method as recited in claim 11, wherein, prior to receiving the message, the at least one identified token is serialized into the security header portion of the message by transforming the at least one identified security token into base 64 encoded data is inherent because this type of encoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of Fieres and de Jong [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 13, the method as recited in claim 12, wherein deserializing comprises an act of converting data from the identified at least one token from base 64 encoding to a byte array is inherent because this type of decoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of Fieres and de Jong [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Claims 15 and 16 are cancelled.

Regarding claim 34 the combined invention of Fieres and de Jong teach the method as recited in claim 1, wherein the one or more security tokens are represented in the message by a markup language identifier [The message includes information for use in generating a token pool, as such this includes token type indicators (US Pub No. 2004/0054628 A1, Pg 6, Par 0101)], and wherein the at least one identified security token is identified by the markup language identifier [Token type indicator specifies format of token – (US Pub No. 2004/0054628 A1, Pg 10, Par 0138)].

Regarding claim 32, the method as recited in claim 14, wherein deserializing comprises an act of converting data from the identified at least one token from base 64 encoding to a byte array is evident because this type of decoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of Fieres and de Jong [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 17, Fieres teach in a computerized network environment including two or more computer systems sending messages through a network communication protocol, a method of sending secure messages using custom security tokens, the method comprising: an act of a sending computer system generating one or more security tokens using one or more corresponding value types [US 6178504 B1, Col 6, Ln 26-38] [US 6178504 B1, Col 14, Table 1], each token including token data that

includes a custom property, wherein the custom property defines one or more of time of day, geographic location, limitations on message access, or limitations on device access [US 6178504 B1, Col 6, Ln 30 –Examiner notes an Application ID contained in a certificate reads on a custom property which defines limitations on message access through classes of services.] [US 6178504 B1, Col 13, Ln 24-32 –Examiner notes COS attributes such as number of usage or expiration time all reading on custom properties.]; an act of encrypting a portion of a message using at least one of the one or more generated security tokens [US 6178504 B1, Col 4, Ln 21-25].

However, Fieres does not explicitly teach the method further comprising an act of inserting the at least one generated security token in an outbound token collection; and an act of converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system.

De Jong teaches in a computerized network environment including two or more computer systems sending messages through a network communication protocol, a method of sending secure messages using custom security tokens, the method comprising: an act of inserting the at least one generated security token in an outbound token collection [Security tokens are organized into chains and or pools. (US 2004/0054628 A1, Pg 7, Par 0140)]; and an act of converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system [(US 2004/0054628 A1, Pg 7,

starting Par 0140) Such a private key is the token pool key, or the token chain key depending on which perspective. Examiner notes that such private keys are securely transported or securely generated as shown in US 2004/0054628 A1, Fig. 19 and 24 and thus are only accessible by sending and receiving entities.].

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the digital content access control of de Jong into the invention of Fieres. The suggestion/motivation would have been to have an invention capable of controlling both application resources and digital content especially when a digital content may require the use of a specific application resource. Fieres and de Jong are analogous because they are both in the same field of endeavor of controlling access in a digital network through the use of security tokens.

Regarding claim 18, the combined invention of Fieres and de Jong teach the method as recited in claim 17, further comprising an act of including one or more digital signatures in the message, wherein the one or more digital signatures are authenticated prior to decrypting the encrypted portion of the message [US 6178504 B1, Col 10, Ln 25-44].

Regarding claim 19, the combined invention of Fieres and de Jong teach the method as recited in claim 17, further comprising an act of including private key information in the message, such that the receiving computer system can access the key from a key provider based on the key information [The Synchronizer is the key provider and

synchronization of token pool information and keys that can be accessed by sending and receiving authenticated digital content request entities through internal requests for synchronization (US 2004/0054628 A1, Pg 18, Par 0213)].

Regarding claim 20, the method as recited in claim 17, wherein the act of converting the token data comprises serializing the token data into base 64 encoding is inherent because this type of encoding is built into the Web Services Security communications protocol and such communications protocol is taught by the combined inventions of Fieres and de Jong [US 2004/0054628 A1, Pg 7, Par 0111-0112].

Regarding claim 21, the combined invention of Fieres and de Jong teach the method as recited in claim 17, wherein the at least one generated security token is a custom security token created using a custom value type, and wherein the custom value type is accessible by both the sending and receiving computer systems [US 6178504 B1, Col 14, Table 1].

Regarding claim 22, the combined invention of Fieres and de Jong teach the the method as recited in claim 17, further comprising an act of creating a signature or encryption function based on the included one or more of a custom property, a signature, and an encryption level in the created binary token [US 6178504 B1, Col 11, Ln 19-24] [US 2004/0054628 A1, Fig 19].

Regarding claims 23 and 24, the combined inventions of Fieres and de Jong teach the method as recited in claim 17, further comprising an act of including a program language value corresponding with each token that is included in the outbound token collection and wherein the program language value is a Common Language Runtime value [(US 2004/0054628 A1, Pg 8, starting Par 0118) du Jong et al. teach "servlet"(s) that can handle the common language infrastructure.]

Claim 25 is cancelled.

Regarding claim 26, the combined inventions of Fieres and de Jong teach the method as recited in claim 17, further comprising an act of assigning the markup language representation of the at least one generated security token a global unique identifier [A global unique identifier is interpreted as a type of identifier known across all platforms or throughout entire network system. Since de Jong's tokens have implementations using URLs, many or all can qualify as a global unique identifier.]

Regarding claim 27 and 28, the combined inventions of Fieres and de Jong teach the method as recited in claim 26, wherein the outbound token collection is a hash table that is keyed by the global unique identifier of the at least one generated security token and wherein the global unique identifier is inserted into a signature or encryption portion of the message [(US 2004/0054628 A1, Pg 10, Par 0140-141) Since the cryptographic

process includes a hashing function, the resulting encryption process can be interpreted as a hashing table since tokens taught by de Jong et al. is also organized in a data structure ie. pools and chains. Many identifiers used by de Jong et al. qualify as the global unique identifier such as the Seed or the last token identifier (since the last token identifier in one embodiment is used to generate the token chain).].

Claim 29 is rejected using references and rationale of claims 17.

Claims 30-31 are cancelled.

Regarding claim 33, the combined invention of Fieres and de Jong teach the method as recited in claim 29, wherein the program language value is a Common Language Runtime value [(US 2004/0054628 A1, Pg 8, starting Par 0118) du Jong et al. teach "servlet"(s) that can handle the common language infrastructure.].

Regarding claim 35, the combined invention of Fieres and de Jong teach the method as recited in claim 17, wherein the act of inserting the at least one generated security token in an outbound token collection further comprises: an act of identifying a markup language representation of the at least one generated security token [Token Chain ID, offset, token type indicator, (Pg 10, Par 0137)], and an act of placing the markup language representation of the at least one generated security token in the outbound

token collection [(US 2004/0054628 A1, Pg 7, starting Par 0140) Such representation is evident in the token pool information.]

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Jeriko P. San Juan whose telephone number is 571-272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

Application/Control Number:
10/645,375
Art Unit: 2132

Page 18


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan

Examiner. Art Unit 2132


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100